

The VPN: Internet Security That Knows No Bounds

A White Paper Prepared by WatchGuard Technologies, Inc.

WatchGuard Technologies, Inc.

316 Occidental Avenue South, Suite 300

Seattle, Washington 98104

<http://www.watchguard.com>

October, 1997

The VPN: Internet Security That Knows No Bounds

Overview

Remote access to a corporate network poses a security threat that can be met with many solutions. From a combination of user IDs and passwords to dedicated leased lines or Virtual Private Networks (VPNs), security for a network extended beyond the walls of headquarters can represent a wide range of costs and varying degrees of effectiveness. With a VPN, Internet security becomes truly “distance independent,” as well as cost-effective and reliable. A company can protect its intellectual property while allowing users outside its main office to access and transmit confidential information over the Internet. At the same time, use of the VPN does not restrict communication over the public, or untrusted, network. WatchGuard Technologies extends the protection of its WatchGuard security system with VPNs for mobile remote users and outside offices.

Extending the Network beyond Your Walls

A Trend Based on Rewards

Exchanging information over the Internet between corporate headquarters and remote users—individuals or offices—can either enhance or subvert a company’s operations. For most companies, the outcome depends on whether that information remains protected at all times. Protecting a corporate network from external hackers and internal abuse presents a tough challenge, but it becomes more complex when the Internet is used to extend the internal network, or intranet, beyond office walls.

Many companies have chosen to deploy laptop computers with modems to create “virtual offices” that include mobile workers such as sales people and tele-commuters. In fact, 20 percent of the employees of medium and large-sized companies rely on portable computers and the number is expected to jump to 28 percent by next year (BRG Newsletter, February 1997). Another key trend is toward the inclusion of trading partners in the corporate network.

Companies such as Mobil Oil, Ford Motor Company and Countrywide Home Loans demonstrate the powerful financial rewards of the extended internal network, called an extranet. For example, Mobil Oil saves millions annually in telephone charges through an extranet application that allows its 300 lubricant distributors worldwide to submit purchase orders over the Internet instead of by fax. For Mobil Oil, a Virtual Private Network prevents its competitors or other unauthorized Internet users from intercepting orders from its lubricant distributors.

Doing It Safely—Then

In the past, securely linking branch offices to the corporate network occurred one of two ways. In each case, a true private network was established, but at great up-front and continuing expense.

First, secure communication could be accomplished with leased lines between locations that were supported by special data services from a telecommunications vendor and expensive hardware and software. The associated costs made it impractical to include many remote users, including trading partners, in all but the most critical situations. For example, a single T1 connection running across several states can cost thousands of dollars each month.

A second approach, used for lighter traffic loads, was to have branch offices use the regular phone system to dial directly into the corporate network. This typically involved long distance calls and dedicated modems. An employee on the road could also rely on this approach as long as the company maintained a modem bank and kept it up to date.

Doing It Safely—Now

With more companies integrating Internet use into their business, it became apparent that a security solution based on low-cost Internet connectivity could transform commerce.

The concept involves use of the public network, or Internet, to establish a “virtual private network” (VPN) on top of it. With a VPN scheme in place, the branch office or employee in the field can simply connect to a local (Internet Service Provider) ISP and go through the Internet to reach the corporate network. A VPN allows the user to set up a private “conversation” with the home office using their normal Internet connection.

Several categories of remote workers can be covered by VPNs, namely, mobile workers, tele-commuters, branch offices, partners, suppliers, and customers. If you have determined that extending your corporate network could improve joint operations with trading partners, boost performance at branch offices, and make your sales force more productive, ask yourself the following questions:

- Will any confidential information flow to and from the remote users?
- Could your business be harmed if a competitor intercepted the transmissions?

- Would it be inappropriate for all the remote users to be able to access the same information from your main office?

“Yes” answers guide you toward a robust VPN solution. And, although it seems obvious that such security within an extranet is critical, according to *NetGuide* (August 1997), it is “perhaps the most important, and one of the least properly addressed areas.” The challenge involves not only protecting your company’s intellectual property from the public, but also preventing some extranet participants from accessing what others may access freely.

Establishing a Virtual Private Network

VPNs are created through security schemes applied to Internet communications. A virtual network is not physical, but forms on demand through software that establishes a point-to-point session between secure clients. In this sense, VPN connections are like private, controlled phone calls (rather than party lines) into the target servers; they can be set up, managed, and disconnected at will by either party. A VPN makes use of the Internet’s physical base of routers, ATM (asynchronous transfer mode) switches, and digital and analog lines without sacrificing security.

A VPN can involve **encryption** alone, or security of the transmission can be strengthened with the addition of user **authentication** and/or a **firewall**. In brief,

- Encryption transforms data into a form that is unreadable to unauthorized users.
- User authentication verifies the identity of users requesting access to network resources.
- Running the transmission through a firewall adds protection from intrusion and abuse.

The VPN, therefore, has the potential to maintain the confidentiality of the transmission while it ensures that the different users have access only to the data which they are authorized to see. Anyone who cannot be authenticated cannot access the network, and any VPN transmission from a host not authorized by the firewall will be denied.

The WatchGuard VPNs

WatchGuard VPNs combine all three of elements—encryption, authentication and firewall—to ensure the highest level security for an extended network.

The heart of the WatchGuard solutions is the WatchGuard Firebox, a high-performance security appliance housing all core firewall functions. The WatchGuard Firebox is teamed with Security Management System software and modules such as the WatchGuard Branch Office VPN to become the WatchGuard system. For details on the Firebox and the complete WatchGuard security system, please refer to the White Papers entitled “The WatchGuard System: An Internet Security System for Business” and “From Firewall to Firebox: The Emergence of the Internet Security Appliance.”

WatchGuard Branch Office VPN

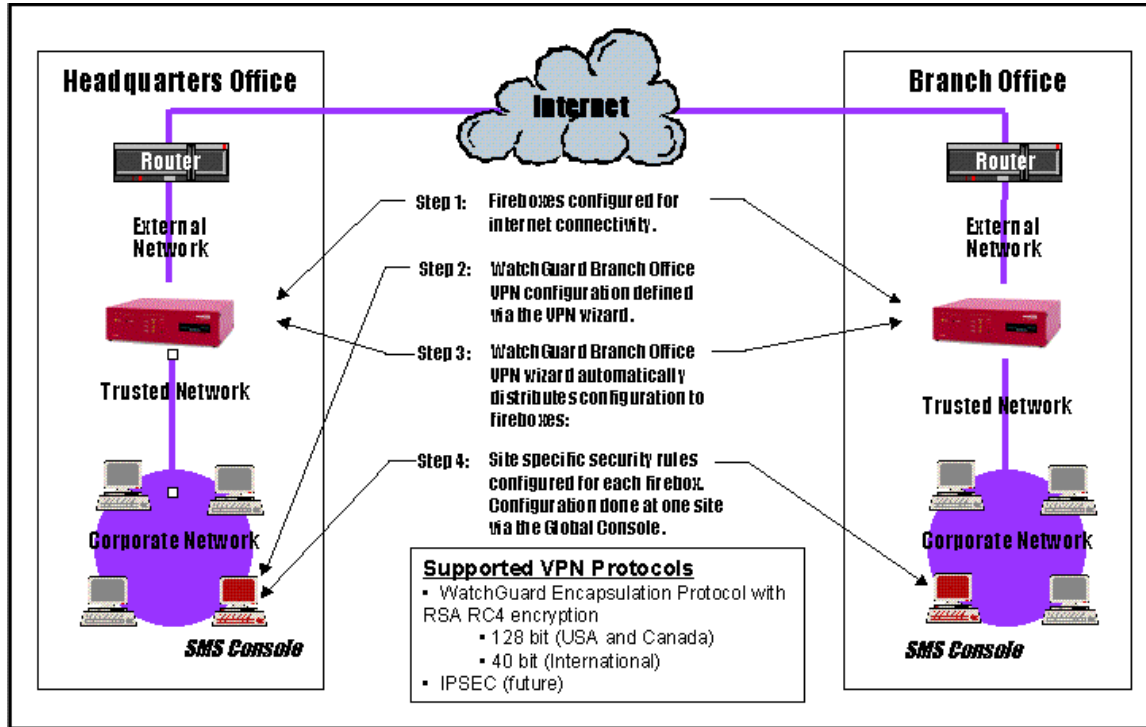
By simply plugging in the WatchGuard Firebox at each location, and adding WatchGuard Branch Office VPN software to each Firebox location, network managers can extend security to all branch offices.

The Fireboxes encrypt all IP packets before sending them over the public networks. This type of connection between the trusted networks or hosts over the public network is known as a “tunnel.” When data passed through this public network—the Internet—is encrypted, the virtual connection is also a private one, making it a virtual private network.

User Authentication is an optional, but highly recommended security layer for the Branch Office VPN that can be implemented with encryption at no additional cost. With Authentication, only authorized users are given access to the network and the system tells those users apart to define appropriate network access. It authenticates users before allowing them through the firewall and attaches a name to their IP address instead of displaying a number, or “machine ID,” such as 165.111.1.99. Reports can then show names of individual users. Security is limited to users that have domain accounts, or that have accounts that have been granted specific access to the network through a trusted domain.

The third security element, running the transmission through a firewall, is an integral part of the WatchGuard system. By configuring the VPN so that traffic is routed through the firewall, security is enforced to a maximum level.

The diagram below illustrates the four-step set-up of the WatchGuard Branch Office VPN.

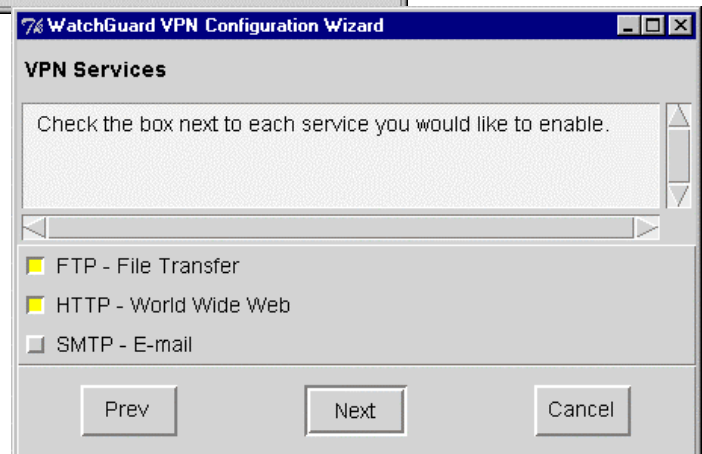
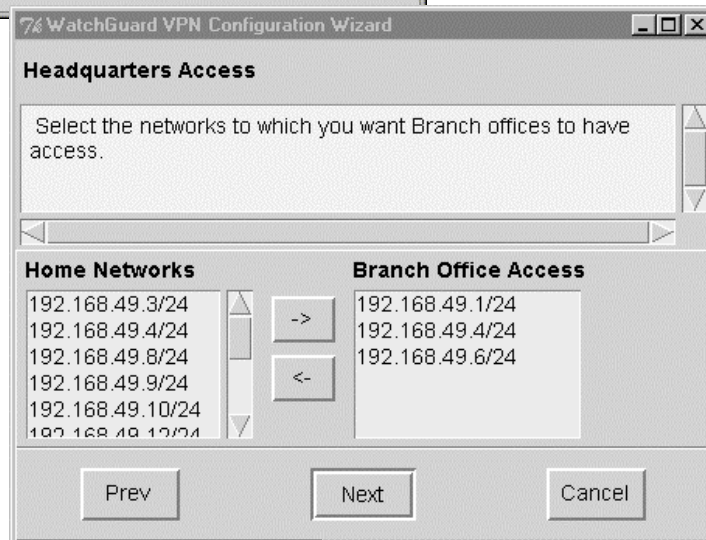


A more detailed explanation of the set up process is as follows:

1. First of all, the branch office must have Internet connectivity. Running WatchGuard Configuration Wizard then allows the network administrator to define the IP addresses for the external (Internet) and trusted (branch office) networks for each branch office Firebox. This configuration can be done before or after the Firebox is installed at the branch office. Fireboxes are installed between the router and Branch Office network at each location.
2. The virtual link between the headquarters Firebox and each branch office Firebox is prepared by configuring the WatchGuard Branch Office VPN software. The Branch Office VPN Wizard facilitates this process in a point-and-click fashion. The VPN configuration addresses three parameters:
 - the headquarters sub-networks that are to be accessible over the VPN.
 - the encryption scheme.

Using the WatchGuard Encapsulation Protocol, the system takes the original IP packets, adds a message authentication code to it, and encrypts it using RSA RC-4 128-bit or 40-bit encryption standards. It then takes the encrypted packet and puts it in a UDP packet for Internet transmission.
 - the services to be made available such as SMTP, FTP, HTTP, and DNS.

The pictures below show how these parameters are input.



Once the configurations are established, the VPN Wizard automatically distributes them via encrypted management sessions between the headquarters and branch office Fireboxes.

3. The user can then do additional configurations for each branch office, establishing site-specific rules and policies. Users also establish how activity will be managed on an ongoing basis—either centrally, using the Global Console, or in a distributed fashion. Global Console resides at only one location in the extended network, and can be used to monitor the entire network protected by the WatchGuard system and WatchGuard Branch Office VPN.

There is a choice whether or not to make the User Authentication option part of the VPN configuration. Configuring User Authentication is straightforward, regardless of whether the system will rely on an NT Authentication Server or the server embedded in the WatchGuard Firebox. If relying on the NT Authentication Server, the IP address or host name of the authentication server is defined as part of the Firebox configuration. It's as simple as telling the Firebox where the server is. If using the embedded server, configuration is just a matter of defining the user names and passwords as part of the WatchGuard setup.

Once the configuration is done, the end-user has nothing special to do to activate it. The following provides an overview of how the authentication process works.

1. The user opens the WatchGuard Authentication URL, which resides on the Firebox, via a Web browser. A Java applet is then invoked and the user enters his/her name and password.



1. The Firebox queries the Authentication Server to validate the user. As authentication is requested, either an NT Domain Authentication Server or the WatchGuard Authentication Server embedded in the Firebox is called on to authenticate the user. If an NT Domain Authentication Server is used, the Firebox transparently queries it for authentication.
2. The Authentication Server determines whether or not the user is authorized for access.
3. The Firebox logs connections and maintains statistics on a per-user basis. If the user is authorized, the Firebox maintains the connection; the browser applet keeps the authenticated session available. If the user is not authorized, the Firebox terminates the connection and alerts the network administrator of an attempted breach.

The benefits of the WatchGuard Branch Office VPN featuring three layers of security—encryption authentication, and firewall—can be summarized as follows. The system:

- provides a secure extension of the corporate network to branch offices;
- uses strong encryption and a unique encapsulation scheme—the WatchGuard Encapsulation Protocol—supporting both the RSA RC-4 128-bit and 40-bit encryption standards to allow safe transmission domestically (128-bit) and internationally (40-bit);
- provides individual user authentication, so management always knows who is attempting to access the network; as a corollary, this enables network administrators to account for branch-office access usage to charge users for access costs and/or to log their activity;
- enables administrators to set up security policies for business partners, as well as internal users, to connect securely to the network.

WatchGuard Remote User VPN

Since one fifth of the employees of medium and large-sized companies rely on portable computers, and the number expected to rise rapidly each year for companies of all sizes, WatchGuard decided to make Remote User VPN a standard part of its security system. Other companies may offer a VPN package for employees on the road, but at additional, and often significant, cost. WatchGuard further simplified and reduced the cost of implementing a mobile-user VPN solution by using a protocol that is widely adopted for laptops. With WatchGuard Remote User VPN the only thing mobile extranet participants have to do is authenticate themselves using a password.

The WatchGuard Remote User VPN eliminates the need to build and maintain local Remote Access Servers, modem banks, dedicated analog lines, and perhaps even toll-free numbers for the company's traveling users and tele-commuters. With the Remote User VPN, laptop users have the option to connect to the corporate network through a local call to an ISP without sacrificing the company's security or ability to control remote connections. Each remote connection is administered, logged, or monitored on an individual basis. With very slight adjustments by both client and administrator, the functionality is the same as with a direct call into the company network. The only difference is that the network session takes place over the Internet, rather than the company's private dial-up network.

The Remote User VPN relies on the widely adopted Point-to-Point Tunneling Protocol (PPTP). Windows NT 4.0 and Windows 95 machines are either equipped with PPTP or are PPTP-ready (can run Dial-up Networking 1.2), so users of the WatchGuard system can have literally no additional costs if they wish to extend their secure network to include mobile workers. Macintosh users can purchase software that gives them the same capability.



Before remote users can access the VPN, the Firebox must be configured to allow access by remote workers. The network administrator simply gives instructions to enable the Remote User VPN through System Management Software that comes standard with the WatchGuard System, identifying the users and their passwords.

For remote users, the process is simple.

1. The remote user establishes connection to the Internet by dialing an ISP or Internet presence. This is no different from any other, routine connection to the Internet
2. A PPTP session is established with the Firebox. Specifically how the user connects to use PPTP depends on the laptop operating system. For Windows 95, access goes through dial-up networking. The brief set-up using the Dial-up Networking package creates a desktop icon so that PPTP sessions are only a click away. After selecting that icon, the remote user then enters a user name and password. In the WatchGuard Remote User VPN, the user name and password are an integral part of establishing an encrypted link, i.e.; user authentication and encryption are tied together because the name and password are used as credentials in creating the encrypted session.

3. The remote user is authenticated via the WatchGuard Remote User Authentication tables.
4. The Remote User VPN connection is then established between the laptop and the corporate network. As that connection is being established, the Firebox automatically negotiates with the laptop to determine the strongest encryption allowable (128-bit or 40-bit). Once the secure link is established, the user has access to all services that Firebox is configured to let him/her have.

In short, after dialing an ISP, the user selects an icon reflecting the Remote User VPN configuration, the user is authenticated (which activates the encryption), then the user is ready for a secure session. All operation is now as if the remote user is directly connected to the LAN, limited only by the speed of the dial-up connection.

Benefits of the WatchGuard Remote User VPN can be summarized as follows:

- is more affordable than its leased-line predecessor for reasons that includes the fact that it uses of common public communication services; is based on widely adopted protocols; and is easily deployed, configured and managed.
- scales well as users are added to the system by relieving the burden of supporting complex, remote access servers and modems;
- maintains secure connections through strong encryption support;
- ensures that only authorized users can access the network;
- involves minimal configuration requirements for the remote user; an employee in the field only has to authenticate him/herself to establish the remote VPN connection;
- enables administrators to set up security policies for remote users, as well as internal users;
- costs nothing extra to establish a Remote User VPN, since the module is part of the standard WatchGuard system, and use of relatively low-cost IP access services make transmissions affordable.

WatchGuard Technologies, Inc. — the Security Appliance Pioneer

WatchGuard Technologies, Inc. designs and produces affordable, easy-to-use Internet security products that enable businesses and schools to conduct safe, secure, and private electronic commerce and communications. In 1996, WatchGuard Technologies pioneered the concept of the high-performance security appliance, now recognized as a trend-setting development in Internet security.

WatchGuard Technologies, Inc. is headquartered in Seattle, Washington USA and is the recognized market leader for affordable next generation Internet/intranet security products.

WatchGuard Technologies, Inc.
316 Occidental Ave. South, Suite 300
Seattle, Washington 98401
USA

Phone: (206) 521-8340
Fax: (206) 521-8341
E-mail: sales@watchguard.com
WWW: <http://www.watchguard.com>

© 1997 WatchGuard Technologies, Inc. All rights reserved. WatchGuard is a trademark of WatchGuard Technologies, Inc. Other names may be trademarks or registered trademarks of their respective companies.